PaloAltoNetworks.PCNSA-JPN.v2020-06-25.q40

試験コード： PCNSA-JPN
試験名称： Palo Alto Networks Certified Network Security Administrator (PCNSA日本語版)
認証ベンダー： Palo Alto Networks
無料問題の数： 40
バージョン： v2020-06-25
ページの閲覧量 :944
問題集の閲覧量 :11661
https://www.jpnshiken.com/shiken/PaloAltoNetworks.PCNSA-JPN.v2020-06-25.q40.html

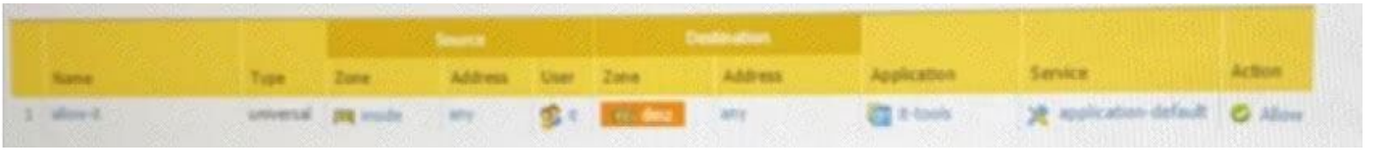
質問: **1**
パロアルトネットワークのファイアウォールを備えたレイヤー3ゾーンの一部であるインターフェースタイプはどれですか？
A. 管理
B. 集計
C. 高可用性
D. 集計
正解: (正解を表示します)

質問: **2**
複数のWindowsドメインコントローラーがある環境でユーザーIDを検出するために使用できるユーザーマッピング方法はどれですか。
A. Active Directoryの監視
B. Windowsクライアントのプローブ
C. Windowsセッションモニタリング
D. ドメインコントローラーの監視
正解: (正解を表示します)

質問: **3**
貴社では、新しいコンプライアンス要件をサポートするために、ワイヤレスデバイスが使用するすべてのIPアドレスの明確なユーザー名属性を要求しています。ワイヤレスデバイス自体のダウンタイムと構成変更を最小限に抑えて、できるだけ早くIPとユーザーのマッピングを収集する必要があります。ワイヤレスデバイスはさまざまな製造元のものです。
シナリオを前提として、IPからユーザーへのマッピングをNGFWに送信するためのオプションを選択します。
A. UID redistribution
B. XFF headers
C. syslog
D. RADIUS
正解: (正解を表示します)

質問: **4**

スクリーンショットに基づいて、含まれているグループの目的は何ですか？



A. ファイアウォールの管理を許可したユーザーのみが含まれます。

B. ファイアウォールの資格情報に基づいて表示されるグループのみです。

C. RADIUS認証サーバーからインポートされるグループです。

D. ユーザー名をグループ名にマップするために使用されます。

正解: **C** (コメントを発表する)

質問: **5**

ファイアウォールは、従業員がYouTubeにアクセスしようとすると、アプリケーションブロックページを送信します。

YouTubeアプリケーションをブロックしているセキュリティポリシールールはどれですか。

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. 許可されたセキュリティサービス

B. intrazone-default

C. ゾーン間デフォルト

D. Googleを拒否

正解: (正解を表示します)

質問: **6**

ホストに感染する新しいマルウェアのグローバル通知を受け取る管理者。感染すると、感染したホストがコマンドアンドコントロール（C2）サーバーに接続しようとします。

ファイアウォールの署名データベースが更新された後、どのセキュリティプロファイルコンポーネントがこの脅威を検出して防止しますか？

A. 送信セキュリティポリシーに適用されるウイルス対策プロファイル

B. インバウンドセキュリティポリシーに適用されるデータフィルタリングプロファイル

C. 送信セキュリティポリシーに適用されるデータフィルタリングプロファイル

D. 受信セキュリティポリシーに適用される脆弱性プロファイル

正解: (正解を表示します)

質問: **7**
会社が1つの建物の1階を占めており、単一のネットワークに2つのActive Directoryドメインコントローラーがある場合、ファイアウォールの管理プレーンはわずかしか使用されません。
ネットワークで十分なユーザーIDエージェントはどれですか？
A. 各ドメインコントローラーに展開されたWindowsベースのエージェント
B. ドメインメンバーの内部ネットワークに展開されたWindowsベースのエージェント
C. ファイアウォールにデプロイされたPAN-OS統合エージェント
D. ネットワーク上に展開されたCitrixターミナルサーバーエージェント
正解: (正解を表示します)

質問: **8**
PAN_OSバージョン9.1以降、セキュリティポリシールールのユーザーフィールド内での使用がサポートされている新しいタイプのオブジェクトはどれですか。
A. 動的ユーザーグループ
B. ローカルユーザー名
C. リモートユーザー名
D. 静的ユーザーグループ
正解: (正解を表示します)

質問: **9**
App-IDの暗黙的な依存関係と明示的な依存関係の2つの違いは何ですか？　2つ選択してください。）
A. 暗黙的な依存関係では、依存アプリケーションをセキュリティポリシーに追加する必要があります
B. 明示的な依存関係では、依存アプリケーションをセキュリティポリシーに追加する必要はありません
C. 明示的な依存関係では、依存アプリケーションをセキュリティポリシーに追加する必要があります
D. 暗黙的な依存関係では、依存アプリケーションをセキュリティポリシーに追加する必要はありません
正解: (正解を表示します)

質問: **10**
WildFireはどのくらいの頻度で動的更新をリリースしますか？
A. 60分ごと
B. 30分ごと
C. 5分ごと
D. 15分ごと

正解: (正解を表示します)

質問: **11**
パロアルトネットワークのファイアウォールで実行中の構成を保存するために使用されるファイルはどれですか？
A. run-configuratin.xml
B. running-config.xml
C. running-configuration.xml
D. run-config.xml
正解: (正解を表示します)

質問: **12**
セキュリティポリシーとセキュリティプロファイルの3つの違いは何ですか？ 3つ選択してください。）
A. セキュリティプロファイルは、それ自体でトラフィックをブロックするために使用されます
B. セキュリティプロファイルはセキュリティポリシーに添付されます
C. セキュリティポリシーはセキュリティプロファイルに添付されます
D. セキュリティプロファイルは許可されたトラフィックでのみ使用する必要があります
E. セキュリティポリシーはトラフィックをブロックまたは許可できます
正解: **B,D,E** (コメントを発表する)

質問: **13**
表示されたセキュリティポリシールールに基づいて、sshはどのポートで許可されますか？

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. 任意のポート
B. sslおよびsnmpv3と同じポート
C. デフォルトのポート
D. 短命なポートのみ
正解: (正解を表示します)

質問: **14**
示されているセキュリティポリシーの例では、どの2つのWebサイトがfckedしましたか？ 2つ選択してください。）

	Name	Tags	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Block-Sites	outbound	Inside	Any	Outside	Any	Any	any	Social-networking	Deny	None

A. YouTube
B. Amazon
C. LinkedIn
D. Facebook
正解: **C,D** (コメントを発表する)

質問: **15**
PowerBall Lotteryは高額の支払い額に達し、会社は従業員が番号を確認できるようにすることで従業員の士気を高めることを決定しましたが、ギャンブルURLカテゴリのブロックを解除したくありません。
従業員が会社がギャンブルURLカテゴリのロックを解除せずにPowerBall宝くじサイトにアクセスできるようにする方法はどれですか。 2つ選択してください。）
A. 許可リストに* .powerball.comを追加します
B. ギャンブルのURLカテゴリからpowerball.comを手動で削除します。
C. PowerBallというカスタムURLカテゴリを作成し、*。powerball.comをカテゴリに追加して、許可するアクションを設定します。
D. powerball.com以外のギャンブルカテゴリのすべてのURLをブロックリストに追加し、ギャンブルカテゴリのアクションを許可に設定します。
正解: (正解を表示します)

質問: **16**
内部ホストが、ソースNATを使用してインターネットのサーバーに接続しようとしています。
ファイアウォールでソースNATを有効にするにはどのポリシーが必要ですか？
A. 外部ソースと任意の宛先アドレスを含むNAT後のポリシー
B. ソースゾーンと宛先ゾーンが指定されたNATポリシー
C. 宛先ゾーンのソースが選択されていないNATポリシー
D. 外部の送信元アドレスと任意の宛先アドレスを持つpre-NATポリシー
正解: (正解を表示します)

質問: **17**
show securityポリシールールに基づいて、内部ゾーンから外部ゾーンへのすべてのFTPトラフィックを照合しますか？
A. 外の入口
B. intercone-default
C. internal-inside-dmz
D. 内部ポータル
正解: **B** (コメントを発表する)

質問: **18**
ファイアウォールが非ローカルアカウントを認証するために外部サービスの複数の認証プロファイルにアクセスするには、何を設定する必要がありますか？
A. 認証リストプロファイル
B. 認証サーバーリスト
C. 認証シーケンス
D. LDAPサーバープロファイル
正解: (正解を表示します)

質問: **19**
URLフィルタリングセキュリティプロファイルのどの2つの項目に対してアクションを設定できますか？ （2つ選択してください。）
A. ブロックリスト
B. カスタムURLカテゴリ
C. PAN-DB URLカテゴリ
D. 許可リスト
正解: **B,C** (コメントを発表する)
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000boO3CAI

質問: **20**
管理者が利用できない更新オプションはどれですか？
A. 新しいURL
B. 新しいアプリケーション署名
C. 新しいスパイウェア通知
D. 新しいウイルス対策署名
E. 新しい悪意のあるドメイン
正解: (正解を表示します)

質問: **21**
ネットワークには、10個のドメインコントローラー、複数のWANリンク、およびミッションクリティカルなアプリケーションをサポートするために必要な帯域幅を備えたネットワークインフラストラクチャがあります。このシナリオで、パロアルトネットワークスはどのタイプのユーザーIDエージェントをベストプラクティスと見なしていますか？
A. キャプティブポータル
B. ドメインコントローラー上のWindowsベースのエージェント
C. 適切なデータプレーンリソースを備えたCitrixターミナルサーバー
D. PAN-OS統合エージェント
正解: **(**正解を表示します**)**

質問: **22**
ベストプラクティスアセスメントに関して正しい説明はどれですか。
A. BPAツールはファイアウォールでのみ実行できます
B. 経験豊富なセールスエンジニアが案内する評価により、予防活動に集中すべき最大のリスクの領域を特定するのに役立ちます
C. 各評価データの採用率を提供します
D. ネットワークとセキュリティアーキテクチャのすべての領域にわたるセキュリティリスク防止のギャップを明らかにするのに役立つ一連のアンケートを提供します
正解: **D (**コメントを発表する**)**

質問: **23**
トポロジーを考慮して、E1 / 1インターフェースをどのゾーンタイプで構成する必要がありますか？
A. レイヤー3
B. タップ
C. 仮想ワイヤー
D. トンネル
正解: **(**正解を表示します**)**

質問: **24**
ファイアウォールを構成できる最小頻度で、新しいwildfireアンチウイルスシグネチャを確認してください。
A. 1分ごと
B. 30分ごと
C. 24時間ごと
D. 5分ごと
正解: **(**正解を表示します**)**

質問: **25**
アプリID更新プロセスのどの時点で、既存のポリシールールがアプリID更新の影響を受けているかを判断できますか？
A. [動的更新]ウィンドウで[新規チェック]をクリックした後
B. アップデートをダウンロードした後
C. ファイアウォール構成を接続した後
D. アップデートのインストール後
正解: **C (コメントを発表する)**

質問: **26**
どの2つのPalo Alto Networksセキュリティ管理ツールが、ポリシーの統合作成、集中管理、集中脅威インテリジェンスを提供しますか。 2つ選択してください。）
A. GlobalProtect
B. Aperture
C. Panorama
D. AutoFocus
正解: **(正解を表示します)**

質問: **27**
攻撃者はサイバー攻撃ライフサイクルのどの段階でPDFファイルを電子メールに挿入しますか？
A. コマンドと制御
B. 偵察
C. インストール
D. 武器化
E. 悪用
正解: **(正解を表示します)**

質問: **28**
統合されたポリシーの作成と集中管理を提供するパロアルトのネットワークセキュリティオペレーティングプラットフォームコンポーネントはどれですか？
A. AutoFocus
B. Prisma SaaS
C. Panorama
D. GlobalProtect
正解: **(正解を表示します)**

質問: **29**
ルールでヒットカウントはどのようにリセットされますか？
A. in the CLI, type command reset hitcount <POLICY-NAME>
B. select a security policy rule, right click Hit Count > Reset

C. Device > Setup > Logging and Reporting Settings > Reset Hit Count
D. with a dataplane reboot
正解: (正解を表示します)

質問: **30**
内部ゾーンと外部ゾーンの間、内部ゾーン内、および外部ゾーン内のトラフィックに一致するセキュリティルールのタイプはどれですか。
A. グローバル
B. ゾーン内
C. ゾーン間
D. ユニバーサル
正解: (正解を表示します)
説明
参照 :https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC

質問: **31**
外部ゾーンと内部ゾーンの間を通過するトラフィックと一致するが、ゾーン内を通過するトラフィックとは一致しないために必要なセキュリティポリシールールはどれですか。
A. グローバル
B. ゾーン間
C. イントラゾーン
D. ユニバーサル
正解: (正解を表示します)

質問: **32**
ある企業が60日前に、古いポートベースのファイアウォールを新しいPalo Alto Networks NGFWに移動しました。ファイアウォールの古いルールまたは未使用のルールを特定するために、会社はどのユーティリティを使用する必要がありますか？
A. ルール使用フィルター>ヒット数> 90日間未使用
B. ルール使用フィルター>未使用のアプリ
C. ルール使用フィルター>アプリが指定されていません
D. ルール使用フィルター>ヒット数> 30日間未使用

正解: **D** (コメントを発表する)

質問: **33**
管理者は、悪意のある横方向の動きにより、ネットワーク内のトラフィックを保護する必要があることに気付きました。表示された画像に基づいて、悪意のある活動を軽減するために管理者はどのトラフィックを監視およびブロックする必要がありますか？
A. 境界トラフィック
B. 南北交通
C. 東西のトラフィック
D. 支社のトラフィック
正解: (正解を表示します)

質問: **34**
別のプロセッサで構成、ロギング、レポート機能を提供するファイアウォールプレーンはどれですか。
A. データ
B. セキュリティ処理
C. ネットワーク処理
D. コントロール
正解: **D** (コメントを発表する)

質問: **35**
USERSゾーンのサーバー管理者は、現在および将来のすべてのパブリッククラウド環境で可能なすべてのサーバーへのSSHアクセスを必要とします。その他の必要な接続はすべて、USERS-とOUTSIDE-zoneの間ですでに有効になっています。Firewall-adminはどのような構成変更を行う必要がありますか？
A. オプションcに加えて、SSHサーバーからの戻りトラフィックが到達できるようにするには、任意のソースIPアドレスから任意の宛先IPアドレスへのアプリケーションSSHのゾーンOUTSIDEからUSERSへの追加ルールが必要です。サーバー管理者
B. アプリケーションSSHの任意の送信元IPアドレスから任意の宛先IPアドレスへのトラフィックを許可するために、ゾーンUSERSからOUTSIDEへのトラフィックを許可するセキュリティルールを作成します
C. destination-port-TCP-22のSERVICE-SSHというカスタムサービスオブジェクトを作成します。ゾーンUSERSとOUTSIDEの間にセキュリティルールを作成して、SERVICE-SSHの任意の送信元IPアドレスから任意の宛先IPアドレスへのトラフィックを許可します
D. オプションaに加えて、source-port-TCP-22を含むSERVICE-SSH-RETURNというカスタムサービスオブジェクトを作成する必要があります。任意の送信元IPアドレスから任意の宛先IPアドレスへのSERVICE-SSH-RETURNのゾーンOUTSIDEからUSERSへのトラフィックを許可する2番目のセキュリティルールが必要です
正解: **B** (コメントを発表する)

質問: **36**
権限を監視し、機密情報のファイルを共有およびスキャンして、Dropboxやsalesforceなどのクラウドベースのアプリケーションを保護するパロアルトのネットワークセキュリティオペレーティングプラットフォームサービスはどれですか。
A. GlobalProtect
B. Prisma SaaS
C. パノラマ
D. オートフォーカス
正解: **B (**コメントを発表する**)**

質問: **37**
セキュリティポリシールールのヒットカウントをどのようにリセットしますか？
A. セキュリティポリシールールを選択し、[ヒットカウント]> [リセット]を選択します。
B. データプレーンを再起動します。
C. 最初にルールを無効にしてから、再度有効にします。
D. CLIコマンドreset hitcount <POLICY-NAME>を入力します。
正解: **(**正解を表示します**)**

質問: **38**
PAN-OS統合USER-IDエージェントを構成するための正しい順序を特定します。
3.サーバーを監視するサービスアカウントを追加します
2.ファイアウォールで監視するサーバーのアドレスを定義します
4.設定をコミットし、エージェントの接続ステータスを確認します
1. User-IDエージェントを実行するのに十分な権限を持つドメインコントローラでサービスアカウントを作成します
A. 1-3-2-4
B. 3-1-2-4
C. 2-3-4-1
D. 1-4-3-2
正解: **(**正解を表示します**)**

質問: **39**
表示されたスクリーンショットに基づいて、どの列にリンクをクリックすると、ポリシールールに一致するすべてのアプリケーションを表示するウィンドウが開きますか？
A. Apps Seen
B. Name
C. Service
D. Apps Allowed
正解: **A (**コメントを発表する**)**

質問: **40**
どのタイプのファイアウォール構成に進行中の構成変更が含まれていますか？
A. 実行中
B. 候補者
C. コミット
D. バックアップ
正解: **(**正解を表示します**)**